UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/612,715	07/01/2003	Luz Maria Soto	010942-0304513	3762

27498 7590 04/02/2009

PILLSBURY WINTHROP SHAW PITTMAN LLP
P.O. BOX 10500
MCLEAN, VA 22102

EXAMINER	
SHAN, APRIL YING	
ART UNIT	PAPER NUMBER
2435	
MAIL DATE	DELIVERY MODE
04/02/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/612,715	SOTO ET AL.	
	Examiner	Art Unit	
	APRIL Y. SHAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *9 December2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) *27 and 28* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on 9 December 2008, PROSECUTION IS HEREBY REOPENED. After careful search, new grounds of rejections are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

2. A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by singing below.

3. Claims 1-28 are pending in the application. Claims 27-28 have been withdrawn from consideration. Thus, claims 1-26 have been examined.

Response to Argument

4. The Applicant's remark/argument regarding Waugh et al. (U.S. Patent No. 6,678,821) in the Appeal brief is summarized as below: Some of them are persuasive and some are not.

a. The Applicant argues: "Waugh does not teach or suggest comparing a collected biometric sample at an authentication server", the examiner found this

argument persuasive. In the below new grounds of rejections Waugh et al. in view of Glass et al., this limitation is addressed. The examiner further notes this combination would predictably result a well known method of biometrically authenticating user by an authentication server over a network. It has been held that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does not more than yield predictable results." *KSR.*, 127 S. Ct. at 1739, 82USPQ2d at 1395 (2007) (citing *Graham*, 383 U.S. at 12).

b. The Applicant argues, "Waugh does not teach or suggest providing a corresponding public key to a service", the examiner respectfully disagrees.

The examiner respectfully directs Applicant's attention to both the title and col. 1, lines 6-10 of Waugh, they disclose "Method and system for restricting access to the private key of a user in **a public key infrastructure**". Further, in col. 1, lines 35-51, Waugh further explains in public key infrastructure, both the senders and the recipient have a pair of keys, a private key and a public key. Both keys are go hand by hand. In other words, the encryption method is asymmetric in a public key infrastructure: if a user's public key was used to encrypt/decrypt a message, then the user's private key must be used to decrypt/encrypt the message. Furthermore, in col. 4, lines 25-37, Waugh teaches "the public key owned by the intended recipient of the encrypted message will often not be stored on the client computer. One way of conveniently allowing use of both private and public keys is to store such keys on servers, such as the ID template server 28 and the certificate authority server 34 respectively. Embedding encryption in the browser facilitates locating and downloading the private and public keys

from the servers on which these keys are stored". From the above cited passages, a person with ordinary skill in the art at the time of the invention would easily understand a corresponding public key provided to a service in a public key infrastructure was taught or suggested in the Waugh reference.

c. The Applicant argues dependent claims are allowable due to dependency, the examiner respectfully disagrees and these arguments are addressed in the below new ground of rejections.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out

the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

8. Claims 1-5, 12-18 and 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Waugh et al. (U.S. Patent No. 6,678,821) in view of Glass et al. (U.S. Patent No. 6,332,193)

As per **claims 1 and 14**, Waugh et al. discloses a method/apparatus ("Method and system for **restricting access to the private key of a user** in a public key infrastructure" – Title) comprising:

storing a private key associated with a user at an authentication server ("(a) storing a plurality of keys; (b)...whether a prospective user of a key in a plurality of keys is the associated user of the key...." – e.g. col. 2, line 65- col. 3, line 3; "one way of conveniently allowing use of both private and public keys is to store such keys on servers – as the ID template server 28 and the certificate authority server 34 respectively...the private keys...from the servers on which these keys are stored" – e.g. col. 4, lines 31-37; "Preferably, for each key in the plurality of keys a biometric standard determined by measuring a selected feature of the associated user is stored in the key storage means" – e.g. col. 2, lines 38-40, "...(a) at least one key storage medium for storing a plurality of keys, each key being useable by an associated user in a public key infrastructure..." – claim 1 and abstract. Please note ID template of the ID template server 28 and the certificate authority sever 34 corresponds to Applicant's an authentication server);

receiving a request for access to a service from the user ("Referring to Fig. 4, there is illustrated a preferred method...of Fig. 1. In step 100, a first user writes or otherwise generates a message that is to be encrypted and sent to a second user. However, the first user does not know his own private key..." – e.g. col. 4, line 65 - col. 5, line 2 and "encryption/decryption might be wholly limited to the client computer itself, or to a computer isolated from any network. The browser might then be used to encrypt documents that are stored on the user's computer to preserve confidentiality" – e.g. col. 7, lines 3-7);

collecting a biometric sample from the user associated via a client associated with the user and remote from the authentication server on a network (e.g. col. 5, lines 3-15); and

if a result of the comparing step indicates a match between the biometric sample and template for the user (step 108 in fig. 4):

allowing the private key from the authentication server to be accessed and used with the request (e.g. col. 5, lines 22-30); encrypting the request with the private key (step 108 in fig. 4 and col. 5, lines 31-33), and

providing the service with access to a public key corresponding to the private key (in col. 1, lines 35-51, Waugh further explains in public key infrastructure, both the senders and the recipient have a pair of keys, a private key and a public key. Both keys are go hand by hand. In other words, the encryption method is asymmetric in a public key infrastructure: if a user's public key was used to encrypt/decrypt a message, then the user's private key must be used to decrypt/encrypt the message. Furthermore, in col. 4,

lines 25-37, Waugh teaches "the public key owned by the intended recipient of the encrypted message will often not be stored on the client computer. One way of conveniently allowing use of both private and public keys is to store such keys on servers, such as the ID template server 28 and the certificate authority server 34 respectively. Embedding encryption in the browser facilitates locating and downloading the private and public keys from the servers on which these keys are stored". From the above cited passages, a person with ordinary skill in the art at the time of the invention would easily understand a corresponding public key provided to a service in a public key infrastructure was taught or suggested in the Waugh reference), wherein access to the private key stored at the authentication server for use in encrypting the user's request is prevented unless and until the authentication server determines that the user's collected biometric sample that was sent by the client matches the biometric template (e.g. step 108 in fig. 4 and col. 5, lines 44-53 and claims 1 and 2).

Although Waugh et al. discloses sending the collected biometric sample from the client to a biometric comparison module, comparing, at the biometric comparison module, the biometric sample to a biometric template associated with the user (e.g. col. 5, lines 15-22), Waugh et al. does not explicitly disclose sending the collected biometric sample from the client to the authentication server and comparing, at the authentication server, the biometric sample to a biometric template associated with the user. However, Glass et al. met the claimed limitation by disclosing *collecting and securely transmitting biometric data over a network. The biometric data is transmitted over a network to an authentication server. Once the biometric data is authenticated, the authenticate server*

then computes a biometric template using the biometric data. This biometric template is then compared to a previously defined biometric template to identify the user and give the user access to a secured resource (e.g. abstract, col. 1, lines 6-10, and col. 3, lines 45-59 of Glass et al.).

Waugh et al. - Glass et al. are analogous art because they are from a similar field of endeavor in authenticating users via biometric samples. Thus, it would have been obvious to a person with ordinary skill in the art, at the time of invention, to modify the teachings of Waugh et al. with sending the collected biometric sample from the client to the authentication server and comparing, at the authentication server, the biometric sample to a biometric template associated with the user taught by Glass et al. The motivation for doing so would have been to provide secure transmission of biometric data to a server at a remote location over a network (e.g. col. 1, lines 6-10 of Glass et al.).

As per **claims 2-3 and 15-16**, Waugh et al. further discloses if the result indicates a match, generating a digital signature using the private key and for use with the request and further providing the digital signature to the service associated with the request (e.g. col. 1, lines 52-55, claim 13 and 27)

As per **claims 4 and 17**, Waugh et al. further discloses providing a biometric signature corresponding to the collected biometric sample to the service associated with the request (e.g. col. 5, lines 7-12).

As per **claims 5 and 18**, Waugh et al. - Glass et al. further discloses comprising: allowing the service to determine whether to fulfill a transaction corresponding to the request in

accordance with the result of the comparing step (e.g. step 108 in fig. 4. Please note "**if there is**..." of Waugh et al. and "This biometric template is then compared to a previously defined biometric template to identify the user and give the user access to a secured resource. The system can be used for online banking and Internet commerce transaction - e.g. abstract of Glass et al.).

As per **claims 12 and 25**, Waugh et al. further discloses comprising: associating user identification information with the private key; and maintaining a digital certificate containing the user identification information and the public key corresponding to the private key at the authentication server (e.g. col. 5, lines3-8 and col. 6, lines 51-56).

As per **claims 13 and 26**, Waugh et al. further discloses wherein the biometric sample includes a fingerprint scan (e.g. col. 5, lines 8-12).

9. Claims 9-11 and 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Waugh et al. (U.S. Patent No. 6,678,821) in view of Glass et al. (U.S. Patent No. 6,332,193) and further in view of Kerr (U.S. Pub. No. 2002/0142844).

As per **claims 9-11 and 22-24**, Waugh et al. – Glass et al. further discloses the collected biometric sample includes integrity information and wherein the integrity information includes a unique transaction identifier (a secret key and transaction token is attached to the digital file – abstract of Glass et al. and col. 5, lines 3-33 and claim 1 of Waugh et al. Please note digital identifier in Waugh et al. corresponds to Applicant's unique transaction identifier) and checking the integrity information included with the biometric sample (e.g. col.5, lines 22-33 and claim 1 of Waugh et al. and abstract of Glass et al.)

Although Waugh et al. – Glass et al. discloses transmission of collected biometric sample in a secure manner, Waugh et al. – Glass et al. does not explicitly disclose encrypting the collected biometric sample for transmission to the authentication server and decrypting the encrypted biometric sample at the authentication server. However, Kerr met the claimed limitation by disclosing in par. [0068] and fig. 4, *a verification system is operatively coupled to network with network interface module. Preferably, the biometric and other user identification information received by the verification system is an encrypted biometric that is decryptable by decryption module.* Please note Kerr's verification system corresponds to Applicant's authentication server.

Waugh et al. - Glass et al. - Kerr are analogous art because they are from a similar field of endeavor in authenticating users via biometric samples. Thus, it would have been obvious to a person with ordinary skill in the art, at the time of invention, to modify the teachings of Waugh et al. – Glass with encrypting the collected biometric sample for transmission to the authentication server and decrypting the encrypted biometric sample at the authentication server taught by Kerr in order to provide secure transmission of biometric data to a server at a remote location over a network.

The examiner further notes this combination would predictably result a well known method of securely transmitting collected user's biometrical sample to an authentication server/system over a network. It has been held that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does not more than yield predictable results." *KSR.*, 127 S. Ct. at 1739, 82USPQ2d at 1395 (2007) (citing *Graham*, 383 U.S. at 12).

10. Claims 6 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Waugh et al. (U.S. Patent No. 6,678,821) in view of Glass et al. (U.S. Patent No. 6,332,193) and further in view of Goldshlag et al. (U.S. Patent No. 6,957,344).

As per **claims 6 and 19**, Waugh et al. – Glass et al. does not discloses generating pre-enrollment keys for the user; supplying the pre-enrollment keys to respective key generators; and generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators, verifying registration of the user in accordance with a comparison of the final enrollment key; creating the biometric template for the user only if registration is verified; and generating the private key only if the biometric template is successfully created associating user identification information with the final enrollment key.

However, the above features are well known in the art. Goldshlag et al. discloses the common user verification features of generating pre-enrollment keys for the user; supplying the pre-enrollment keys to respective key generators; and generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators (*A licensing authority provides key information to manufactures that insert the key information into a trusted devices. The trusted devices generate final private and public keys using the key information* – e.g. abstract and *where the authority preferably produces seed material that the registrant may use to produce a final private/public key pair* – e.g. col. 2, lines 9-12. Please note key information/seed material corresponds to Applicant's pre-enrollment keys and final

private/public keys correspond to Applicant's final enrollment key and further note licensing authority corresponds to Applicant's key generators and manufacture/trusted devices corresponds to Applicant's key administrator. Licensing authority and manufacture/trusted devices are two different entities. Furthermore, since key information is seed material and it has to be inserted correctly before creating final keys) and verifying registration of the user in accordance with a validation of the final enrollment key (e.g. col. 2, lines 12-13)

It would been obvious to a person with ordinary skill in the art at the time of the invention to combine Goldshlag et al.'s above user verification features with Waugh et al. – Glass et al. in order for the authority to produce seed material that the registrant may use to produce a final private/public key pair.

The examiner further notes this combination would predictably result a well known method of two different entities to produce keys to enhance security. It has been held that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does not more than yield predictable results." *KSR.*, 127 S. Ct. at 1739, 82USPQ2d at 1395 (2007) (citing *Graham*, 383 U.S. at 12).

11. Claims 7-8 and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Waugh et al. (U.S. Patent No. 6,678,821) in view of Glass et al. (U.S. Patent No. 6,332,193) and further in view of Goldshlag et al. (U.S. Patent No. 6,957,344) - Brandys (U.S. Patent No. 7,188,362).

As per **claims 7-8 and 20-21**, Waugh et al. – Glass et al. - Goldshlag et al. does not disclose creating the biometric template for the user only if registration is verified; and generating the private key only if the biometric template is successfully created associating user

identification information with the final enrollment key. However, this well-known feature is disclosed in Brandys (e.g. col. 2, lines 32-38, col. 3, lines 42-53 and claim 1).

It would have been obvious to a person with ordinary skill in the art to combine the well-known features of Brandys' with Waugh et al. – Glass et al. - Goldshlag et al. motivated by a need for new and improved systems for authenticating messages. The system should analyze biometric information as provided by the user as part of the authentication process. The system should also include features to safeguard the keys that are used in the authentication process.

The examiner further notes this combination would predictably result a well known method of creating the biometric template for the user only if registration is verified; and generating the private key only if the biometric template is successfully created associating user identification information with the final enrollment key. It has been held that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does not more than yield predictable results." *KSR.*, 127 S. Ct. at 1739, 82USPQ2d at 1395 (2007) (citing *Graham*, 383 U.S. at 12).

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. However, applicants are **strongly urged** to consider the cited references carefully and distinguish them from the instant claims in accordance with 37CFR 1.111c when presenting an amendment in response to the current Office Action.

- Sweet et al. (U.S. Pub. No. 2002/0031230) teaches a server holds all PKI private keys and certificates used fro encryption or signing, the user's security profile, including credential and biometric templates.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to APRIL Y. SHAN whose telephone number is (571)270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/April Y Shan/
Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435